



一种基于二进制序列的秘密共享新方法

程叶霞^{1,2}, 杜跃进^{1,3}, 杨凯², 何申², 彭晋², 姜文⁴

(1. 中国科学院信息工程研究所 北京 100093;

2. 中国移动通信研究院安全技术研究所 北京 100053;

3. 阿里巴巴集团安全部 北京 100102; 4. 国家计算机网络应急技术处理协调中心 北京 100029)

摘要:提出了一种与传统的秘密共享方法不同的新型的秘密共享方法,该方法是基于二进制秘密序列的位运算的秘密共享方法。秘密包括但不限于密码、消息等,秘密序列包括但不限于密码序列、消息序列等,将采用非 M 序列法则法形成的非 M 序列作为其秘密共享的子秘密序列 M' 的构成元素。提出了基于二进制序列的秘密共享的子秘密生成方法及对应的秘密恢复方法,该方法具有可行性与实效性。

关键词:秘密共享;二进制序列;非 M 序列;门限方案;秘密恢复;信息安全

doi: 10.11959/j.issn.1000-0801.2015251

A Novel Secret Sharing Method Based on Binary Sequence

Cheng Yexia^{1,2}, Du Yuejin^{1,3}, Yang Kai², He Shen², Peng Jin², Jiang Wen⁴

(1. Institute of Information Engineering, China Academy of Sciences, Beijing 100093, China;

2. Department of Security Technology, China Mobile Research Institute, Beijing 100053, China;

3. Security Department, Alibaba Group, Beijing 100102, China;

4. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China)

Abstract: A novel secret sharing method was proposed based on binary sequence, which was quite different from the traditional secret sharing method. This secret sharing method was based on binary secret sequence using bit operations. The secret here included but not limited to key, message, etc, meanwhile the secret sequence included but not limited to key sequence, message sequence and so on. And two new concepts which were called non- M sequence and non- M sequence rule method were defined. By using the non- M sequence rule method, the elements of sub-secret sequence M' of secret sharing were computed. The method for generating sub-secrets and the method for recovering secret was proposed based on binary sequence. The method was practical and effective.

Key words: secret sharing, binary sequence, non- M sequence, threshold scheme, secret recovery, information security

收稿日期:2015-06-17;修回日期:2015-09-23

基金项目:国家自然科学基金资助项目(No.61171173),国家高技术研究发展计划(“863”计划)基金资助项目(No.2011AA01A103),国家发展和改革委员会信息化领域创新能力建设专项(网络安全应急技术国家工程实验室项目)资助项目

Foundation Items: The National Natural Science Foundation of China(No.61171173),The National High Technology Research and Development Program of China (863 Program) (No. 2011AA01A103),The National Development and Reform Commission Innovation Capacity Building Project of Information Area Fund(NELCERT)

论文引用格式:程叶霞,杜跃进,杨凯等.一种基于二进制序列的秘密共享新方法.电信科学,2015251

Cheng Y X, Du Y J, Yang K, et al. A novel method for secret sharing based on binary sequence. Telecommunications Science, 2015251



1 引言

随着计算机网络和通信技术的迅速发展,信息安全问题日益突出。现代密码学技术在保证信息的机密性、完整性、可用性、可靠性和不可否认性方面都具有重要作用。其中,秘密共享机制是密码管理机制和分权机制的一个核心部分。

对于目前的计算机系统和通信系统而言,大量的机密信息以文档的形式存储于计算机中,并依据不同的类型和密级使用不同的密钥去保护它们。通常为了便于管理大量的密钥,使用的全部密钥可能又被一个主密钥来保护,最终导致存储在系统中的所有信息的安全可能取决于一个主密钥。主密钥成为整个系统的安全关键点,如果将它交给单独的一个管理员保管,可能造成一些难以克服的弊端。首先,这个管理员将会具有同他保管的主密钥一样的安全敏感性,需要重点保护,如果他保管的主密钥意外丢失或者他本人遭遇不测,整个系统可能就无法使用了。其次,这个管理员的个人素质和他对组织的忠诚度将成为系统安全的关键,如果他为了某种利益而将他保管的主密钥主动泄露给他人,将会危害整个系统的安全。

能够解决上述问题的方法称为秘密共享,此处的秘密包括但不限于密码、消息、文件信息、通信信息等,它将一个秘密信息(包括主密钥等)进行分权分责处理,从而得到多个子秘密,并将多个子秘密分别交由多个组织或用户共同保管,而且只有多个组织或用户将自己的份额都放在一起,才能够恢复出所共享的秘密,否则无法恢复出秘密。秘密共享一方面有利于防止权力过分集中,另一方面可以保证秘密的安全性和完整性。

因此,本文从秘密共享的方法自身出发,提出了一种与传统的秘密共享方法不同的新型秘密共享方法,这也是本文的主要创新点所在。该方法是基于二进制秘密序列的位运算的秘密共享方法,秘密包括但不限于密码、消息等,秘密序列包括但不限于密码序列、消息序列等,将采用非 M 序列法则形成的非 M 序列作为其秘密共享的子秘密序列 M' 的构成元素,并提出了基于二进制序列的秘密共享的子秘密生成方法及对应的秘密恢复方法。实验证明该方法具有可行性与实效性,同时该方法为秘密共享方法提供了新的思路与举措,大大扩展了秘密共享方法的应用范围,具有灵活性和可控性,并且在抗抵赖性上和密码管理方面具有实用价值。

2 相关研究

当前在秘密共享方面的研究侧重于可验证的秘密共享、秘密份额的有效分发、秘密共享方案的应用场景,比如指纹模糊金库、用户管理、数据保护等。秘密共享的技术方案有很多种,最简单的就是秘密分割,其思想很简单,当不想将一个十分贵重的东西的命运完全寄托于某一个人时,可以把它分成很多份,每一份交付给一个人,当然单独的每一份没有什么价值,只有将所有份额放到一起才能重构价值。其他复杂的秘密共享方法包括:拉格朗日插值多项式门限方案、矢量门限方案、高级门限方案、同余类方案、矩阵法方案等^[1-6]。

国外研究方面,参考文献[1]中,Shamir利用有限域上的多项式方程结合Lagrange插值公式构造了一个 (t,n) 门限方案。参考文献[2]中,Blakley利用关于空间中的点的知识提出了秘密共享方案,即若将共享秘密映射到 t 维空间中的一个点,且根据共享秘密构造的每一个秘密份额都是包含这个点的 $t-1$ 维超平面的方程,那么利用 t 个或 t 个以上的这种超平面的焦点刚好确定这个点。参考文献[3]提出了一种能够有效识别骗子的 (t,n) 门限方案。参考文献[4]提出了一种基于位平面变换和布尔运算的新型秘密共享方案。

国内研究方面,李慧贤等人^[7]于2008年提出了利用双线性对构造可证明安全的密码共享方案的新方法。石润华等人^[8]于2012年提出了一种基于Stern-Brocot树的秘密共享方案。宋云等人^[9]于2013年提出了基于极小线性码上的秘密共享方案,给出了极小线性码的构造方法,并研究了极小线性码的判别条件,给出所构造的密码共享方案的极小授权子集。于佳等人^[10]于2014年提出了一种无可信中心的可公开验证的多秘密共享方案。殷凤梅等人^[11]于2015年提出了一种 (t,n) 门限追踪匿名认证方案。荣辉桂等人^[12]于2015年提出了一种基于Shamir秘密共享的密钥分发与恢复算法。

3 基于二进制序列的秘密共享新方法

本文所提出的基于二进制序列的秘密共享新方法是基于二进制秘密序列的位运算的秘密共享方法。其中,秘密包括但不限于密码、消息等,秘密序列包括但不限于密码序列、消息序列等。

3.1 基于二进制序列的秘密共享方案流程

基于二进制序列的秘密共享方案的流程包括多个步骤,其方案流程如图1所示。

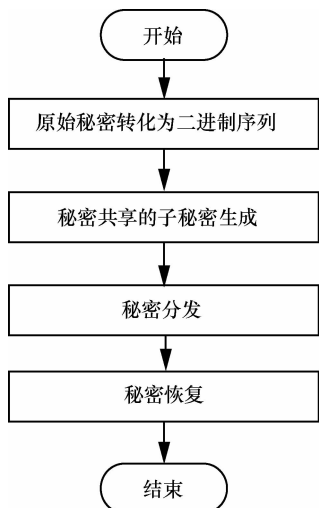


图1 基于二进制序列的秘密共享方案流程

由图1可知,其秘密共享方案包括以下几个步骤。

第1步,原始秘密转化为二进制序列,即给出原始的秘密信息,并进行预处理转化为对应的二进制秘密序列。如果给出的原始秘密信息为二进制秘密序列,则采用原始的二进制秘密序列;如果给出的原始的秘密信息不是二进制格式,则需要预处理,转化为对应的二进制秘密序列。由于该步骤比较简单,不再进行详细介绍。

第2步,秘密共享的子秘密生成,即根据共享人数生成对应的子秘密。这是秘密共享新方法的核心关键。具体方法会在第3.2节进行详细介绍。

第3步,进行秘密的分发,即将生成的子秘密分发给共享的人员。

第4步,如果后续需要,则进行秘密恢复,即根据共享人员的子秘密恢复出原始秘密。具体方法将在第3.3节中进行详细介绍。

3.2 秘密共享的子秘密生成方法

经过基于二进制序列的秘密共享方案流程的第1步,得到二进制秘密序列。此处进行如下假设,进而做出相应的定义。

假设1 假设秘密序列 M 是二进制序列,其位数为 n 位,即 $M=m_n m_{n-1} \cdots m_2 m_1$,且其中 m_i 等于0或1。

定义1 (非 M 序列)非 M 序列是针对秘密序列 M 而言其秘密共享的子秘密序列 M' 的构成元素,即: $M'=m'_n m'_{n-1} \cdots m'_2 m'_1$,且其中 m'_i 等于0或1,并至少存在一个 $m'_i \neq m_i$,即秘密序列的 n 位二进制中至少有1位与原来位的值不同。

定义2 (非 M 序列法则) 根据上述非 M 序列的定义

所形成的非 M 序列的原理则称为非 M 序列法则。

定义3 (非 M 序列法则法) 非 M 序列法则法是指利用上述非 M 序列法则形成非 M 序列的方法。

规则1 通过非 M 序列法则生成的子秘密序列,只有其秘密共享的子秘密序列 M' 均在一起时才能够恢复出秘密 M 。后续第3.3节会给出对规则1的证明过程。

在上述定义的基础上,下面详细阐述基于二进制序列的秘密共享的子秘密生成方法。该生成方法的过程如图2所示,包括以下5个步骤。

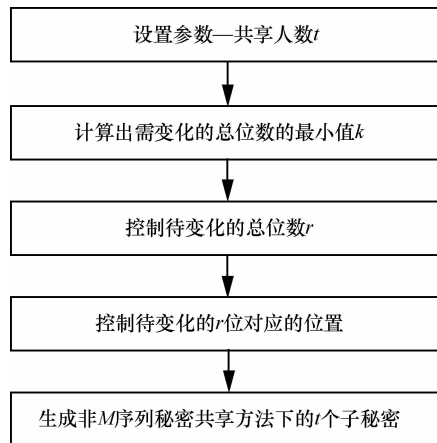


图2 基于二进制序列的秘密共享的子秘密生成方法

由图2可知,具体的基于二进制序列的秘密共享的子秘密生成方法包括以下步骤。

步骤1 设置参数—共享人数 t 。根据实际的秘密共享方案的需要,设置秘密共享的人数 t ,作为输入参数进行参数设置。

步骤2 计算出需变化的总位数的最小值 k 。由于步骤1设置的共享人数为 t ,依据非 M 序列法则,设 k_i 为实数,则存在方程 $2^{k_i}-1=t$,解方程可得 $k_i=1b(t+1)$ 。

那么需变化的总位数的最小值 k (k 为整数)的取值状况根据 k_i 的值的性质可分为以下两种情况。

- 当 $k_i=1b(t+1)$ 为小数时,则需对其进行向上取整,因此 $k=\lceil 1b(t+1) \rceil$ 。
- 当 $k_i=1b(t+1)$ 为整数时,则 $k=1b(t+1)$,又因为对于整数而言,其值本身与向上取整的值之间存在相等关系,即 $1b(t+1)=\lceil 1b(t+1) \rceil$,因此进一步可得到 $k=1b(t+1)=\lceil 1b(t+1) \rceil$ 。

综上所述,则 $k=\lceil 1b(t+1) \rceil$,即需变化的总位数的最小值 k 为 $\lceil 1b(t+1) \rceil$,也即 $1b(t+1)$ 向上取整的结果。



步骤 3 控制待变化的总位数 r 。由步骤 2 得到需变化的总位数的最小值 $k=\lceil \lg(t+1) \rceil$, 同时由于秘密序列是 n 位的二进制序列, 因此待变化的总位数 r 的取值范围为 $[k, n]$, 即 $k \leq r \leq n$, 可以在该范围之内自定义地控制待变化的总位数 r 。

令 $r=k+p$, 则 $p \geq 0$ 且 $p \leq n-k$ 。依据 p 和 t , 可分为以下 3 种状况分析。

- $p=0$ 且 $\lg(t+1)$ 为整数时的状况。
- $p=0$ 且 $\lg(t+1)$ 为小数时的状况。
- $0 < p \leq n-k$ 时的状况。

步骤 4 控制待变化的 r 位对应的位置。由步骤 3 得出待变化的总位数为 r , 那么针对位数为 n 位的二进制秘密序列 $M=m_n m_{n-1} \cdots m_2 m_1$ 而言, 其位置的选择方案共有 C_n^r 种, 即从第 1、2、3、 $\cdots$ 、 $n-1$ 、 n 位中任取 r 位作为变化的对应位置。因此, 待变化的 r 位对应的位置可以自定义控制。不妨假设这 r 个待变化的位置分别对应第 α_1 位、第 α_2 位、 $\cdots$ 、第 α_{r-1} 位、第 α_r 位, 其中 $\alpha_1 < \alpha_2 < \cdots < \alpha_{r-1} < \alpha_r$ 。

步骤 5 生成非 M 序列秘密共享方法下的 t 个子秘密。由于步骤 4 确定待变化的 r 位对应的位置为第 α_1 位、第 α_2 位、 $\cdots$ 、第 α_{r-1} 位、第 α_r 位, 其中 $\alpha_1 < \alpha_2 < \cdots < \alpha_{r-1} < \alpha_r$ 。同时根据假设 1、定义 1、定义 2、定义 3 可知, 秘密序列 M 是二进制序列, 其位数为 n 位, 即 $M=m_n m_{n-1} \cdots m_2 m_1$, 且其中 m_i 等于 0 或 1。则将非 M 序列作为其秘密共享的子序列 M' 的构成元素, 即: $M'=m_n' m_{n-1}' \cdots m_2' m_1'$, 且其中 m_i' 等于 0 或 1, 并至少存在一个 $m_i' \neq m_i$, 即秘密序列的 n 位二进制中至少有 1 位与原来位的值不同。因此, 对于待变化的 r 位对应位置为第 α_1 位、第 α_2 位、 $\cdots$ 、第 α_{r-1} 位、第 α_r 位所构成的二进制序列 $m_{\alpha_1} m_{\alpha_2} \cdots m_{\alpha_r}$, 共有 2^r-1 个不同的二进制序列 $m_{\alpha_1}' m_{\alpha_2}' \cdots m_{\alpha_r}'$, 使得 $m_{\alpha_1}' m_{\alpha_2}' \cdots m_{\alpha_r}' \neq m_{\alpha_1} m_{\alpha_2} \cdots m_{\alpha_r}$ 。将 $n-r$ 个不变的位数与变化的 r 位按位置组合之后得到 n 位二进制序列 $m_n' m_{n-1}' \cdots m_2' m_1'$, 从而得到 $M=m_n m_{n-1} \cdots m_2 m_1$ 序列在秘密共享下的 2^r-1 个子秘密, 分别记为二进制序列 $SSM_1, SSM_2, SSM_3, \cdots, SSM_{2^r-2}, SSM_{2^r-1}$, 同时把这 2^r-1 个子秘密所构成的集合记为子秘密集 SSM_Set , 因此, $SSM_Set=\{SSM_1, SSM_2, SSM_3, \cdots, SSM_{2^r-2}, SSM_{2^r-1}\}$ 。

再从 SSM_Set 集合中自定义地控制并选择出 t 个作为子秘密进行后续的秘密分发, 这 t 个子秘密分别记为 $SSM_Chosen_1, SSM_Chosen_2, SSM_Chosen_3, \cdots, SSM_Chosen_{t-1}, SSM_Chosen_t$, 其构成的集合记为 SSM_Chosen_Set , 因此, $SSM_Chosen_Set=\{SSM_Chosen_1, SSM_Chosen_2, SSM_Chosen_3,$

$\cdots, SSM_Chosen_{t-1}, SSM_Chosen_t\}$, $SSM_Chosen_Set \subseteq SSM_Set$ 。并将剩余的 2^r-1-t 个子秘密作为秘密共享恢复的要素和后续秘密分发的备份要素予以保存, 这 2^r-1-t 个子秘密分别记作 $SSM_UnChosen_1, SSM_UnChosen_2, SSM_UnChosen_3, \cdots, SSM_UnChosen_{2^r-2-t}, SSM_UnChosen_{2^r-1-t}$, 其构成的集合记为 $SSM_UnChosen_Set$, 因此, $SSM_UnChosen_Set=\{SSM_UnChosen_1, SSM_UnChosen_2, SSM_UnChosen_3, \cdots, SSM_UnChosen_{2^r-2-t}, SSM_UnChosen_{2^r-1-t}\}$, $SSM_UnChosen_Set \subseteq SSM_Set$ 。同时, 上述 3 个集合之间存在如下关系: $SSM_Chosen_Set + SSM_UnChosen_Set = SSM_Set$ 。

综上, 步骤 5 生成其秘密共享方法下的子秘密, 需要依据 r, k 和 t 分为以下 3 种状况分析。

- 当 $r=k$ 且 $\lg(t+1)$ 为整数时, 则依据非 M 序列法则直接计算出 t 个子秘密, 进行后续的秘密分发。
- 当 $r=k$ 且 $\lg(t+1)$ 为小数时, 则依据非 M 序列法则, 计算出 2^k-1 个子秘密, 并从中选出 t 个子秘密进行后续的秘密分发, 剩余的 2^k-1-t 个子秘密用作秘密恢复时的要素和秘密分发的备份要素, 加以保存。
- 当 $k < r \leq n$ 时, 则依据非 M 序列法则, 计算出 2^r-1 个子秘密, 并从中选出 t 个子秘密进行后续的秘密分发, 剩余的 2^r-1-t 个子秘密加以保存, 用于后期秘密恢复时的要素和秘密分发的备份要素。

3.3 秘密恢复方法

经过基于二进制序列的秘密共享方案流程的第 2 步, 生成了基于二进制秘密序列的秘密共享的子秘密, 并通过方案流程的第 3 步, 将第 2 步所生成的 t 个子秘密分发给共享的 t 个人。此处作如下假设, 进而作出相应的规则证明与恢复方法。

假设 2 假设 t 个共享人员被分发到的子秘密分别记作 $S_1, S_2, S_3, \cdots, S_{t-1}, S_t$ 。

假设 3 假设在方案流程第 2 步子秘密生成过程中未被分发而被保存的 2^r-1-t 个子秘密分别记作 $R_1, R_2, R_3, \cdots, R_{2^r-2-t}, R_{2^r-1-t}$ 。

由规则 1 可知, 通过非 M 序列法则生成的子秘密序列, 只有其秘密共享的子秘密序列 M' 均在一起时才能够恢复出秘密 M 。

根据定义的非 M 法则, 结合位运算的知识, 研究出其对应的秘密恢复方法为将秘密共享的所有子秘密序列 M' 进行按位异或运算, 运算后的结果即秘密 M 。

针对上述情况,即 t 个被分发的子秘密 $S_1, S_2, S_3, \dots, S_{t-1}, S_t$ 和 2^r-1-t 个未被分发而被保存的子秘密 $R_1, R_2, R_3, \dots, R_{2^r-2-t}, R_{2^r-1-t}$ 均在一起时才能够恢复出秘密 M , 而且恢复的方法为将这 t 个被分发的子秘密 $S_1, S_2, S_3, \dots, S_{t-1}, S_t$ 和 2^r-1-t 个未被分发而被保存的子秘密 $R_1, R_2, R_3, \dots, R_{2^r-2-t}, R_{2^r-1-t}$ 进行按位异或运算, 即 $M=S_1 \oplus S_2 \oplus S_3 \oplus \dots \oplus S_{t-1} \oplus S_t \oplus R_1 \oplus R_2 \oplus R_3 \oplus \dots \oplus R_{2^r-2-t} \oplus R_{2^r-1-t}$ 。

下面对规则 1 进行证明。

证明 由非 M 序列的定义可知, 非 M 序列是针对秘密序列 M 而言其秘密共享的子秘密序列 M' 的构成元素, 即: $M'=m_n' m_{n-1}' \dots m_2' m_1'$, 且其中 m_i' 等于 0 或 1, 并至少存在一个 $m_i' \neq m_i$, 即秘密序列的 n 位二进制中至少有 1 位与原来位的值不同。其中秘密序列 M 是二进制序列, 其位数为 n 位, 即 $M=m_n m_{n-1} \dots m_2 m_1$, 且 m_i 等于 0 或 1, 因此, $S_1, S_2, S_3, \dots, S_{t-1}, S_t$ 和 $R_1, R_2, R_3, \dots, R_{2^r-2-t}, R_{2^r-1-t}$ 共同形成针对 r 位进行非 M 序列法则变化后的 2^r-1 个序列。把这 2^r-1 个序列统计编号记为 $T_1, T_2, T_3, \dots, T_{2^r-2}, T_{2^r-1}$, 其中任意的 $T_i=t_{n,i} t_{n-1,i} \dots t_{2,i} t_{1,i}$, 且 $t_{j,i}$ 等于 0 或 1, 并且满足 $t_{j,i}=m_i$ 或 $\neg m_i$ 成立, 所以 $S_1 \oplus S_2 \oplus S_3 \oplus \dots \oplus S_{t-1} \oplus S_t \oplus R_1 \oplus R_2 \oplus R_3 \oplus \dots \oplus R_{2^r-2-t} \oplus R_{2^r-1-t} = T_1 \oplus T_2 \oplus T_3 \oplus \dots \oplus T_{2^r-2} \oplus T_{2^r-1}$ 。

同时, 由于异或运算等价于模 2 加法运算。因此存在:

$$\begin{aligned} & T_1 \oplus T_2 \oplus T_3 \oplus \dots \oplus T_{2^r-2} \oplus T_{2^r-1} \\ &= t_{n,1} t_{n-1,1} \dots t_{2,1} t_{1,1} \\ & \oplus t_{n,2} t_{n-1,2} \dots t_{2,2} t_{1,2} \\ & \oplus t_{n,3} t_{n-1,3} \dots t_{2,3} t_{1,3} \\ & \oplus \dots \\ & \oplus t_{n,2^r-2} t_{n-1,2^r-2} \dots t_{2,2^r-2} t_{1,2^r-2} \\ & \oplus t_{n,2^r-1} t_{n-1,2^r-1} \dots t_{2,2^r-1} t_{1,2^r-1} \\ &= \sum_{i=1}^{2^r-1} t_{n,i} \bmod 2 \sum_{i=1}^{2^r-1} t_{n-1,i} \bmod 2 \dots \sum_{i=1}^{2^r-1} t_{2,i} \bmod 2 \sum_{i=1}^{2^r-1} t_{1,i} \bmod 2 \end{aligned}$$

由于发生变化的总位数为 r 位, 不妨假设后 r 位发生了变化。对于其他变化位按此情形可同理证明。因此继续证明。

对于前 $n-r$ 位未发生变化的位而言, 当 $r+1 \leq j \leq n$ 时,

$$\begin{aligned} \text{则 } \sum_{i=1}^{2^r-1} t_{j,i} \bmod 2 &= \sum_{i=1}^{2^r-1} m_{j,i} \bmod 2。 \text{ 其中当 } m_{j,i}=m_j=0 \text{ 时,} \\ \sum_{i=1}^{2^r-1} m_{j,i} \bmod 2 &= 0; \text{ 当 } m_{j,i}=m_j=1 \text{ 时, } \sum_{i=1}^{2^r-1} m_{j,i} \bmod 2 = 1。 \text{ 因此,} \\ \sum_{i=1}^{2^r-1} m_{j,i} \bmod 2 &= m_j, \text{ 进而得到 } \sum_{i=1}^{2^r-1} t_{j,i} \bmod 2 = m_j。 \end{aligned}$$

对于后 r 位发生变化的位而言, 当 $1 \leq j \leq r$ 时, 则

$$\sum_{i=1}^{2^r-1} t_{j,i} \bmod 2 = (\neg m_j) \cdot 2^{r-1} + m_j \cdot (2^{r-1} - 1) \bmod 2 = m_j \cdot (2^{r-1} - 1) \bmod 2 = m_j。$$

综合上述证明, 则:

$$\begin{aligned} & T_1 \oplus T_2 \oplus T_3 \oplus \dots \oplus T_{2^r-2} \oplus T_{2^r-1} \\ &= \sum_{i=1}^{2^r-1} t_{n,i} \bmod 2 \sum_{i=1}^{2^r-1} t_{n-1,i} \bmod 2 \dots \sum_{i=1}^{2^r-1} t_{2,i} \bmod 2 \sum_{i=1}^{2^r-1} t_{1,i} \bmod 2 \\ &= m_n m_{n-1} \dots m_2 m_1 \\ &= M \end{aligned}$$

所以, $S_1 \oplus S_2 \oplus S_3 \oplus \dots \oplus S_{t-1} \oplus S_t \oplus R_1 \oplus R_2 \oplus R_3 \oplus \dots \oplus R_{2^r-2-t} \oplus R_{2^r-1-t} = T_1 \oplus T_2 \oplus T_3 \oplus \dots \oplus T_{2^r-2} \oplus T_{2^r-1} = M$ 。命题得证。证毕。

因此, 通过对所有 2^r-1 个子秘密进行异或运算即可进行秘密恢复, 即 $M=S_1 \oplus S_2 \oplus S_3 \oplus \dots \oplus S_{t-1} \oplus S_t \oplus R_1 \oplus R_2 \oplus R_3 \oplus \dots \oplus R_{2^r-2-t} \oplus R_{2^r-1-t} = T_1 \oplus T_2 \oplus T_3 \oplus \dots \oplus T_{2^r-2} \oplus T_{2^r-1}$ 。

4 实例与结果分析

根据第 3 节所给出的秘密共享的新方法, 本文给出了实例并获取了相应的结果。以原始秘密序列为二进制序列 $M=10101111$ 为例, 把右边第 1 位定义为第 1 位, 左边第 1 位定义为第 8 位。因此, 共 8 位, 即 n 均为 8。实例的具体过程分别如下。

第 1 组实例设置参数—共享人数 t 为 3, 计算出 $k_i=2$, $k=2$, 进而取 $p=1$, 得到控制待变化的总位数 $r=3$, 进而自主选择出待变化的 3 位分别为第 1、2、3 位, 即右边 3 位。生成的所有 7 个子秘密集合 SSM_Set 为 $\{10101011, 10101101, 10101110, 10101001, 10101010, 10101100, 10101000\}$, 任意选取其中 3 个 (分别为 10101011、10101101、10101110) 分发给共享人员, 因此 $SSM_Chosen_Set=\{10101011, 10101101, 10101110\}$, 剩余的 4 个子秘密形成 $SSM_Chosen_Set=\{10101001, 10101010, 10101100, 10101000\}$ 。

最后由子秘密进行秘密恢复, $10101011 \oplus 10101101 \oplus 10101110 \oplus 10101001 \oplus 10101010 \oplus 10101100 \oplus 10101000 = 10101111 = M$ 。

第 2 组实例设置参数—共享人数 t 为 4, 计算出 $k_i=2$, $32, k=3$; 进而取 $p=0$, 得到控制待变化的总位数 $r=3$; 进而自主选择出待变化的 3 位分别为第 1、7、8 位, 即右边 1 位, 左边 2 位; 生成的所有 7 个子秘密集合 SSM_Set 为 $\{00101111, 11101111, 10101110, 01101111, 00101110,$



11101110, 01101110}, 任意选取其中 4 个 (00101111、11101111、10101110、01101111) 分发给共享人员, 因此 $SSM_Chosen_Set = \{00101111, 11101111, 10101110, 01101111\}$, 剩余的 4 个子秘密形成 $SSM_Chosen_Set = \{00101110, 11101110, 01101110\}$ 。

最后由子秘密进行秘密恢复, $00101111 \oplus 11101111 \oplus 10101110 \oplus 01101111 \oplus 00101110 \oplus 11101110 \oplus 01101110 = 10101111 = M$ 。

综合实例过程与结果可知, 基于二进制序列的秘密共享新方法在秘密共享的子秘密生成与秘密恢复方面都是可行并有效的, 具有实际应用效果。

5 结束语

本文从秘密共享的方法自身出发, 提出了一种与传统的秘密共享方法不同的新型的秘密共享方法——基于二进制序列的秘密共享新方法。这也是本文的主要创新点所在。该方法是基于二进制秘密序列的位运算的秘密共享方法, 秘密包括但不限于密码、消息等, 秘密序列包括但不限于密码序列、消息序列等, 采用非 M 序列法则形成的非 M 序列作为其秘密共享的子秘密序列 M' 的构成元素, 并提出了基于二进制序列的秘密共享的子秘密生成方法及对应的秘密恢复方法。实例证明该方法具有可行性与实效性。

同时该方法的优点主要体现在以下几方面: 第一, 基于二进制秘密序列的位运算的秘密共享方法, 其中非 M 序列法则对应的秘密共享的空间大, 具有灵活性和抗抵赖性; 第二, 该方法可以结合分组运算等操作, 与传统的秘密共享方法迭代使用, 具有很好的扩展性; 第三, 该方法中, 用户可以根据自己的需求对多个过程参数进行自主控制; 第四, 本文所提出的秘密共享方法为秘密共享方法提供了新的思路与举措, 大大扩展了秘密共享方法的应用范围, 具有灵活性和可控性, 并且在抗抵赖性上和密码管理方面具有实用价值。

参考文献

- 1 Shamir A. How to share a secret. Communications of the ACM, 1979, 24(11): 612~613
- 2 Blakley G. Safeguarding cryptographic key. Proceedings of AFIPS 1979 National Computer Conference, New York, USA, 1979: 313~317
- 3 Luon-Chang L. A (t,n) threshold secret sharing system with efficient identification of cheaters. Computing and Informatics,

2005, 24(12): 529~541

- 4 Gyan S Y, Aparajita O. A novel multi secret sharing scheme based on bit plane flips and Boolean operations. Proceedings of the 48th Annual Convention of Computer Society, Jabalpur, India, 2014: 765~772
- 5 Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE Transactions on Information Theory, 1983, 30(2): 208~210
- 6 Karnin E D, Greene J W, Hellman M E. On sharing secret systems. IEEE Transactions on Information Theory, 1983, 29(1): 3~41
- 7 李慧贤, 庞辽军. 基于双线性变换的可证明安全的秘密共享方案. 通信学报, 2008, 29(10): 45~50
Li H X, Pang L J. Provably secure secret sharing scheme based on bilinear maps. Journal on Communications, 2008, 29(10): 45~50
- 8 石润华, 黄刘生, 杨威等. 新型有效的秘密共享方案. 通信学报, 2012, 33(1): 10~16
Shi R H, Huang L S, Yang W, et al. Novel and effective secret sharing scheme. Journal on Communications, 2012, 33(1): 10~16
- 9 宋云, 李志慧, 李永明. 基于极小线性码上的秘密共享方案. 电子学报, 2013, 41(2): 220~226
Song Y, Li Z H, Li Y M. Secret sharing schemes based on minimal linear codes. Acta Electronica Sinica, 2013, 41(2): 220~226
- 10 于佳, 陈养奎, 郝蓉等. 无可信中心的可公开验证多秘密共享. 计算机学报, 2014, 37(5): 1030~1038
Yu J, Chen Y K, Hao R, et al. Publicly verifiable multi-secret sharing without trusted centers. Chinese Journal of Computers, 2014, 37(5): 1030~1038
- 11 殷凤梅, 侯整风, 濮光宇等. (t,n) 门限追踪匿名认证方案. 计算机工程, 2015, 41(5): 149~152
Yin F M, Hou Z F, Pu G N, et al. (t, n) threshold tracing anonymous authentication scheme. Computer Engineering, 2015, 41(5): 149~152
- 12 荣辉桂, 莫进侠, 常炳国等. 基于 Shamir 秘密共享的密钥分发与恢复算法. 通信学报, 2015, 36(3): 60~69
Rong H G, Mo J X, Chang B G, et al. Key distribution and recovery algorithm based on Shamir's secret sharing. Journal on Communications, 2015, 36(3): 60~69

[作者简介]



程叶霞, 女, 中国科学院信息工程研究所博士生, 中国移动通信研究院网络与信息安全研究员, 主要研究方向为网络攻防、网络安全、信息安全、移动互联网安全。



杜跃进,男,中国科学院信息工程研究所教授、博士生导师,阿里巴巴集团安全技术副总裁,主要研究方向为网络安全、移动互联网安全。哈尔滨工业大学(威海)、北京邮电大学、公安大学兼职教授。拥有 15 年网络安全工作经验,推动了我国网络安全应急响应力体系的建设,曾任网络安全应急技术国家工程实验室主任、国家网络信息安全技术研究所所长等职,是北京奥运会、上海世博会、广州亚运会等大型活动的最高层网络安全专家。主持多项国家重大科研项目,获得国家科技进步奖一等奖两次,入选国家新世纪百千万人才工程,并获得国务院特殊津贴。



何申,男,中国移动通信研究院安全技术研究所所长助理,主要研究方向为网络安全、移动互联网安全。



彭晋,男,中国移动通信研究院安全技术研究所副所长,主要研究方向为网络安全、移动互联网安全。



杨凯,男,中国移动通信研究院网络与信息安全研究员,主要研究方向为网络攻防、网络安全、移动互联网安全。



姜文[通信作者],男,国家计算机网络应急技术处理协调中心高级工程师,主要研究方向为基础设施安全、信息安全、电力系统及其自动化。